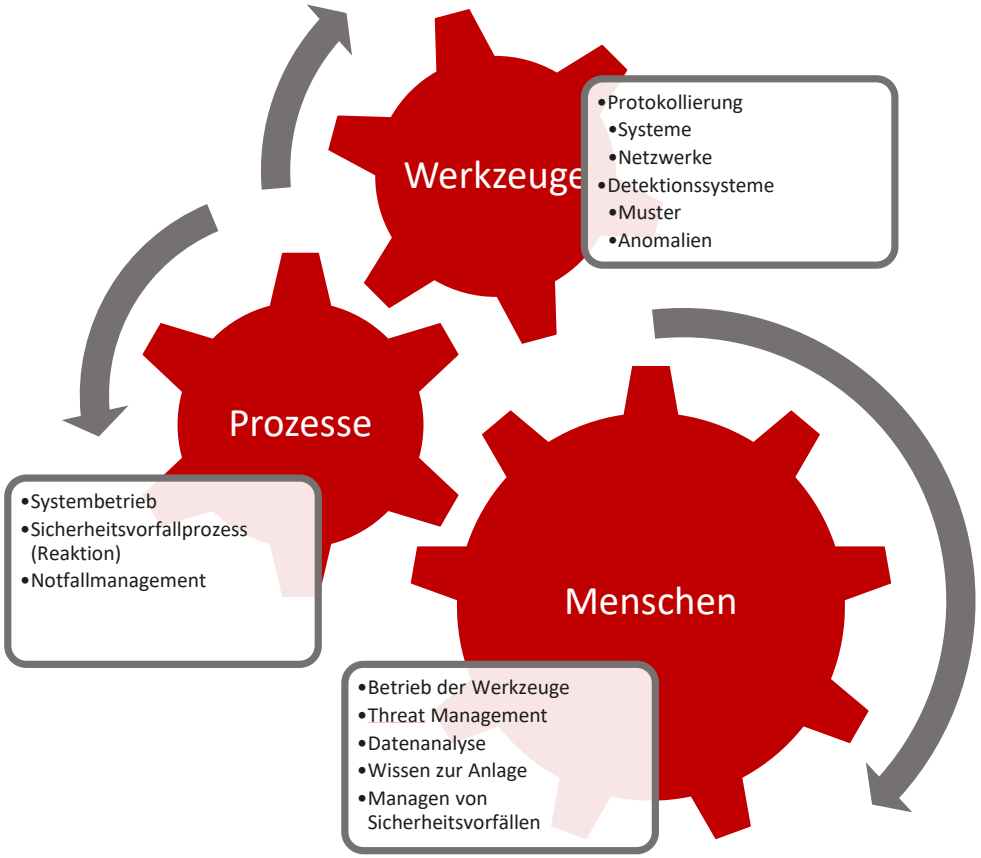
Digitale Technologien bieten die Möglichkeit Prozesse besser zu verstehen und Daten zu gewinnen, um Entscheidungen besser treffen zu können. Wie Dr. Caradot, unser Interviewpartner, sagt: „Digitale Lösungen sind Begleiter, um die Situation besser zu verstehen, aber können keine investiven Maßnahmen ersetzen." Digitale Technologie können viel Mehrwert in der Wasserwirtschaft bieten – Monitoring von Überläufen und Grundwasserständen, einfachere Auslesung von z. B. Wasserzählern, verbessterte Kanalinspektion mittels Künstlicher Intelligenz. Aber neben dem Mehrwert, den sie bieten, bringen sie auch neue Gefahren mit sich. Die Cybersicherheit ist ein Thema, das keinesfalls unterschätzt werden darf. So beginnt die Fokusstrecke dieser Ausgabe mit Systemen zur Angriffserkennung und geht dann auf verschiedene Aspekte der Digitalisierung und Automatisierung in der Wasserwirtschaft ein.

Digitalisierung und Automatisierung

Systeme zur Angriffserkennung in der Leit- und Fernwirktechnik

Die Erkennung und Behandlung von Cyberangriffen in Leit- und Fernwirktechnik ist aufgrund der Verpflichtung im IT-SiG 2.0 aktuell ein heißes Thema bei Versorgungsunternehmen. Der folgende Artikel zeigt auf, welche gesetzlichen Vorgaben für ein System zur Angriffserkennung für KRITIS-Betreiber existieren. Zudem enthält er Vorschläge zur Planung und Umsetzung eines solchen Systems und beleuchtet den Nachweisprozess.

Die Erkennung und Behandlung von Cyberangriffen in der Leit- und Fernwirktechnik von Energie- und Wasserversorgern ist seit dem IT-SiG 2.0 [1] ein vieldiskutiertes Thema. Es gibt erhebliche Unterschiede bei den Vorstellungen, welche Werkzeuge, Prozesse und Betriebsleistungen erforderlich sind. Große Versorgungsunternehmen tun sich hier leicht ein Arsenal an State of the Art IT-Security Überwachungswerkzeugen in eigenen Security Operations Centern zu betreiben. Mittelständische Betreiber verfügen oft weder über die finanziellen Mittel noch genügend Personal, um einen solchen Betrieb zu leisten. Parallel argumentieren findige Softwarehersteller mit niedrigsten Betriebsaufwänden aufgrund angeblich künstlich intelligenter Produkte.



Quelle: ausecus GmbH

Bild 1: Bestandteile eines Angriffserkennungssystems

Für viele steht der 1. Mai 2023 als gesetzliche Frist für die Einführung und teilweise auch den Nachweis im Raum. Neben der Herausforderung sich mit einem komplexen neuen Thema und einem undurchdringlich anmutenden Informationsdschungel verschiedener Anbieter auseinanderzusetzen, herrscht auch Zeitdruck.
Der folgende Artikel soll über die gesetzlichen Anforderungen und eine mögliche Nachweisführung mehr Aufschluss geben. Außerdem soll er dabei helfen, die verschiedenen Dienstleistungsangebote zu unterscheiden.

Ein System zur Angriffserkennung ist…

Ein System zur Angriffserkennung (SzA), wie es vom BSIG (§ 2 Abs. 9b, § 8a Abs. 1) [2] und EnWG (§ 11 Abs. 1e) [3] von Betreibern Kritischer Infrastrukturen und Energieverteilungsnetzen bis Mai 2023 (BSIG § 8a Abs. 1a, EnWG § 11 Abs 1f) [siehe 2 und 3] verlangt wird, ist ein System aus Werkzeugen, Prozessen und Spezialisten. Geeignete Betriebsparameter sollen mit angemessenem Aufwand nach Stand der Technik automatisiert untersucht werden. Cyberangriffe sollen dabei nicht nur erkannt, sondern auch behandelt werden. Nur so entsteht ein konkreter Sicherheitsmehrwert (**Bild 1**).
Versorgungsunternehmen die nach BSIG (§ 8a) zertifiziert sind, haben wohl den zeitlichen Vorteil, dass Sie den Nachweis im nächsten, dem 1. Mai 2023 folgenden, regulären Audit mit erbringen dürfen. Dennoch entbindet sie das sicherlich nicht davon, ein solches System rechtzeitig in Betrieb zu haben, z. B. hinsichtlich der Haftungsfrage.
Manche Versorgungsunternehmen unterliegen der gesetzlichen Pflicht noch nicht, da sie die in der KRITIS-V festgelegten Schwellenwerte unterschreiten. Allerdings wird die nationale Umsetzung der europäischen NIS-2 Richtlinie [4] für 2024 erwartet. Durch die darin vorgegebenen branchenspezifischen Kennwerte, wie Umsatz oder Mitarbeiterzahl, wird sich der Kreis der KRITIS-Betreiber erheblich vergrößern. Insofern sollte auch hier das Thema SzA auf die Tagesordnung gesetzt werden.
Ein gängiges Missverständnis bei einem SzA ist, dass mit der Beschaffung und Installation einer Software für Intrusion Detection (IDS) und/oder Logmanagement bzw. Security Information & Event Management (SIEM) diese Anforderung erfüllt werden kann. Um das zu vermeiden, konkretisiert das BSI die Auslegung mit der Orientierungshilfe (OH).

Die Orientierungshilfe des BSI – mehr als nur eine Orientierungshilfe?

Die OH [5] als Interpretationshilfe der Gesetzesvorgaben wurden bereits mit deren Veröffentlichung zum 1. April 2021 angekündigt. Am 29. August 2022 hat das BSI die OH veröffentlicht (**Bild 2**).
In der OH beschreibt das BSI die Bestandteile eines Systems zur Angriffserkennung und klassifiziert die Elemente und Ausbaustufen in MUSS, SOLL und KANN. Anhand der Prüfung und, wenn möglich, Anwendung dieser Komponenten kann ein Umsetzungsgrad gemessen werden. Am Ende des Dokuments wird eine angemessene Umsetzung der gesetzlichen Anforderungen anhand konkreter Umsetzungsgrade beschrieben. Die Orientierungshilfe verliert damit den Charakter einer Empfehlung und wird vielmehr zur de-facto Methode für eine gesetzeskonforme Umsetzung. Allerdings

Bild 2: Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

gibt es genau dazu gerade einen intensiven Dialog zwischen BSI, Verbänden und Zertifizierern. Im Falle, dass man seine individuelle Anwendung eines SzA zwar innerhalb der gesetzlichen Vorgaben, aber nicht im Umfang der OH implementieren will, ist eine nachvollziehbare und gut dokumentierte Begründung für die Nachweisführung beim Auditor des Zertifizierers unbedingt erforderlich. Kernargumente sind hier die im Gesetz verankerte Angemessenheit und ein gut geführtes Risikomanagement, um nachzuweisen, dass bestimmte Maßnahmen an manchen Stellen nicht erforderlich sind. Unabhängig davon, ob manche der Ausprägungsgrade vielleicht nicht an jeder Stelle gleichermaßen erforderlich erscheinen, ist die OH ein gut verständliches Best-Practice-Dokument, welches die ideale Herangehensweise für Cyberangriffserkennung in Versorgungsunternehmen beschreibt.
Auf folgende Punkte wird in der OH besonderes Augenmerk gelegt:

- Vollumfängliche Planung: Auch wenn Systeme/Daten bei der Angriffserkennung keine oder vorerst keine Berücksichtigung finden, ist das zu dokumentieren und zu begründen.
- Erfassung und Analyse von Systemprotokolldaten und Netzwerkprotokolldaten,
- aktives Sammeln und systematisches Auswerten von Angriffsinformationen für die automatische Angriffserkennung und das Schwachstellenmanagement,

Tabelle 1: Im ersten Nachweiszyklus reicht der Umsetzungsgrad 3

Umsetzungsgrad	Planung	MUSS	SOLL	KANN	KVP
0					
1	umgesetzt	in einzelnen Bereichen			
2		unvollständig			
3 1. Nachweis		umgesetzt	geprüft		geplant
4 2. Nachweis			umgesetzt oder ausgeschlossen		wird gelebt
5				umgesetzt	wird gelebt

Quelle: ausecus GmbH

ausreichend fachkompetentes Personal für die Analyse der Angriffsmeldungen,
umfänglicher Notfallmanagementprozess (Reaktion).

Bestandteile eines Systems zur Angriffserkennung

Analog zur Beschreibung der OH kann ein System zur Angriffserkennung in folgende Bestandteile aufgegliedert werden:

Datenerfassung (Protokollierung): Die Erfassung relevanter Protokolldaten der betreffenden Systeme und Netzwerke, die Aufschluss über einen Cyberangriff geben können.

Detektion: Die Durchsuchung der Protokolldaten nach geeigneten Hinweisen auf sicherheitsrelevante Ereignisse, wie mögliche Angriffe oder Schwachstellen.

Reaktion: Der angemessene Umgang mit entdeckten sicherheitsrelevanten Ereignissen.

Wie geht man das Thema an?

Der Umfang eines solchen Systems, bei dem technische Werkzeuge lediglich ein Bestandteil sind, wird gerne unterschätzt. Auch ohne die Vorgabe der Orientierungshilfe muss ein solches Vorgehen mit einer Planung begonnen werden, aus der die erforderlichen Werkzeuge und deren Betriebsmodell hervorgehen.

Da es oft bereits vorhandene Protokollierungs- und Erkennungsmaßnahmen gibt, ist es ratsam, sich im ersten Schritt einen Überblick über den erforderlichen Umfang einer Planung und der umzusetzenden Maßnahmen zu verschaffen. Dann wird schon absehbar, ob ein Berater mit bestimmtem Erfahrungshintergrund hinzugezogen werden sollte oder welche Optionen beim Betrieb der Werkzeuge in Frage kommen.

Vorgehensweise einer Planung

Prüfung aller relevanten Datenquellen (Systeme und Netzwerke) und zu erfassenden Daten anhand des Risikomanagements (Angriffsvektoren, Eintrittswahrscheinlichkeiten, Schadenshöhen) und der Netzwerkstrukturpläne,
Prüfung der zentralen Auswertbarkeit der Daten (Datenformate, verfügbare Hard- und Softwareschnittstellen),
Festlegung von entsprechenden Speicherdauern und entstehenden Speichervolumen,
Beachtung der DSGVO- und BetrVG-Anforderungen,
Festlegung der Erkennungsmethoden anhand der Angriffsvektoren,
Festlegung eines Prozesses für die systematische und regelmäßige Erfassung und Integration von Angriffsdaten in die Erkennungsmethodik,
Festlegung des gewünschten Betriebsmodells (Leistungen selbst erbringen oder zukaufen). Bei der Nutzung von Dienstleistern, Definition der Schnittstellen,
Prüfung und gg.f Ergänzung der vorhandenen Notfallmanagement-Prozesse.

Vorgehensweise Umsetzung

Abhängig vom Betriebsmodell, Auswahl der Werkzeuge bzw. Dienstleister,
Aufbau der erforderlichen Personalorganisation,
Implementierung der Prozesse,
Implementierung eines Kontinuierlichen Verbesserungsprozess (KVP) – Ein System zur Angriffserkennung erfordert im Betrieb eine kontinuierliche Verbesserung, um effizient und wirksam zu funktionieren,
Durchführung von Übungen zur Feststellung und Verbesserung der Wirksamkeit.

Make or Buy Entscheidung

Je nach Auslastung des Informationssicherheitsverantwortlichen (ISB) ist der Einsatz eines Beraters bei der Planung eine hilfreiche Komponente. Es ist ratsam hierbei darauf zu achten, dass idealerweise Erfahrung für genau diese Tätigkeit und ein entsprechender Hintergrund (ISMS für Betreiber des entsprechenden Sektors) vorhanden ist.

Bei der Umsetzung bietet sich der Einsatz von Dienstleistern für kleine und mittelständische Betreiber an, da im Regelfall das vorhandene Personal in anderen Aufgaben gebunden ist. Hinzu kommt, dass der Aufbau einer erforderlichen Personalorganisation weder wirtschaftlich sinnvoll noch kurzfristig umsetzbar ist.

Hier stellt sich die Frage des Betriebsmodells. Soll der Dienstleister die Überwachungssysteme lediglich betreiben, heißt sich um die Verfügbarkeit und Aktualität aller Komponenten kümmern? Oder soll der Dienstleister die Alarme und Meldungen analysieren? Möglicherweise soll er die Leistung ganzheitlich erbringen und die dafür nötigen Komponenten mitbringen. Letzteres hat den Vorteil, dass die Verantwortlichkeiten damit eindeutig festgelegt werden.

Wichtig ist, dass die erhobenen Daten aus der Leittechnik diese nicht verlassen. Das heißt, Datenverarbeitung und Datenhaltung

sollte nur innerhalb derselben Infrastruktur erfolgen. Der Einsatz eines Dienstleisters erfolgt dann über sichere Fernzugriffsverfahren (Verschlüsselung, Multi-Faktor-Authentisierung). So führt eine Kompromittierung beim Dienstleister nicht automatisch dazu, dass die Leittechnikdaten im Darknet wiederzufinden sind.
Weitere Details zu Komponenten und der Umsetzung sind in Angriffserkennung in [6] beschrieben.

Nachweisverfahren

Prüfungsberechtigte

Prüfungsberechtigt sind laut Nachweisdokument P* Teil PS.A im Idealfall die üblicherweise eigesetzten Zertifizierer und deren Auditoren. Dem ist so, weil ein SzA in §8a eingefügt wurde und damit Bestandteil des §8a Nachweises ist. Für Energieanlagen und Energieversorgungsnetze gemäß EnWG ist die Akkreditierung nach EnWG §11 Abs. 1a/1b (IT-Sicherheitskatalog der Bundesnetzagentur) erforderlich.

Prüfungsverfahren

Im Nachweisdokument P* [7, 8] ist der Nachweis im Umsetzungsgradverfahren der OH abgebildet.
Wie die Auditoren den Status ermitteln, kann unterschiedlich erfolgen – beispielsweise in Form eins Interviews oder als Self-Assessment mittels Fragebogen und einer nachfolgenden Prüfung.
Es ist ratsam sich mit den Auditoren im Vorfeld über das Prüfungsverfahren auszutauschen.
Abweichungen werden ebenso im Teil PD.E des Nachweisdokuments P* [7, 8] festgestellt und dokumentiert. Dabei wird zwischen geringfügigen Abweichungen und schwerwiegenden oder erheblichen Abweichung bzw. Sicherheitsmängeln unterschieden.
Auch hier ist es sinnvoll mit den Auditoren im Vorfeld zu sprechen.
Durch Lieferschwierigkeiten der für die Datenerhebung erforderlichen Hardwarekomponenten beispielsweise, können sich erhebliche Verzögerungen ergeben. Hier hilft die Einschätzung des Auditors, um Konflikte zu vermeiden (s. **Tabelle 1**).

Fazit

Ein System zur Erkennung von Cyberangriffen in Leit- und Fernwirktechnik von Versorgungsunternehmen ist ein absolut sinnvoller Beitrag für die Resilienz unserer Volkswirtschaft. Es dient zur Absicherung gegenüber einer immer stärker werdenden Bedrohung durch Kriminelle und staatliche Akteure. Insofern ist diese Maßnahme des IT-SiG 2.0 sehr zu begrüßen.
Die unkonkrete Formulierung im Gesetzestext und die späte Konkretisierung in der OH des BSI, 17 Monate nach Gesetzesveröffentlichung und nur sieben Monate vor dem Nachweisdatum, verursacht wenig hilfreichen Stress. Das ist insbesondere bei den kleineren und mittleren Betreibern so. Versorgungsunternehmen haben längere Planungs- und Budgetierungszyklen, leiden unter dem Fachkräftemangel in besonderem Maße und haben mit der Energiekrise gerade mehr als genug zu tun.
Diese Stress-Situation treibt viele Betreiber in die Arme von Produktverkäufern, die ihnen Soft- und Hardware verkaufen, die angeblich keinen Betriebsaufwand verursachen, nie ausfallen und deren Sicherheitsmeldungen immer verständlich und eindeutig sind. Sie verkaufen quasi Gesetzeskonformität aus der Packung. Unter normalen Umständen würde das niemand glauben, aber wenn die Zeit drängt und keine alternative Lösung greifbar ist, erscheint das manchen als eine gute Idee. Der traurige Nebeneffekt ist, dass derartige Systeme dann tatsächlich auch erst mal „funktionieren".
Hier wäre sinnvoller, das Thema trotz Personal- und Zeitmangel geplant anzugehen und, wenn erforderlich, Abweichungen in Kauf zu nehmen. Es ist anzunehmen, dass dieses Vorgehen vom BSI akzeptiert wird, wenn ein fundierter Umsetzungsplan erkennbar ist.
Abgesehen davon hat sich das BSI zum 1. Mai 2023 mit weit über 1.000 Einreichungen auseinanderzusetzen. Hier ist auch unklar, bis wann man eine Antwort auf seinen Nachweis erhält. Das BSI wird hier sicherlich Versorger, die nichts einreichen oder keinerlei Umsetzung durchgeführt haben, zuerst bedienen.

Literatur

[1] IT-SiG 2.0, Bundesgesetzblatt Jahrgang 2021 Teil 1 Nr. 25.

[2] BSI-Gesetz §8a 1a), BSI-Gesetz §2 9b): https://www.gesetze-im-internet.de/bsig_2009/

[3] Energiewirtschaftsgesetz – EnWG §11 1d): https://www.gesetze-im-internet.de/enwg_2005/index.html

[4] NIS-2: https://www.consilium.europa.eu/de/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

[5] Veröffentlichung OH zum Einsatz von SzA, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf

[6] Angriffserkennung in Leit- und Fernwirktechnik als Dienstleistung, vgbe energy journal 09/22

[7] BSI Nachweisdokument P* nach BSIG: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Nachweisdokument_P.html

[8] BSI Nachweisdokument P* nach EnWG: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/nachweisdokument-p-enwg.html

[9] BSI Nachweisdokument KI*: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/nachweisdokument-ki-enwg.pdf

Autor:
Sascha Jäger
Geschäftsführer
ausecus GmbH
www.ausecus.com
info@ausecus.com
0821 207097-0